

09/46525 30.06.98

日本国特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

REC'D	14 AUG 1998
WIPO	PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office. 2

出願年月日  
Date of Application: 1997年 6月30日

出願番号  
Application Number: 平成 9年特許願第173672号

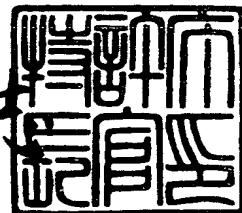
出願人  
Applicant(s): 日本電信電話株式会社  
エヌティティエレクトロニクス株式会社

PRIORITY DOCUMENT

1998年 7月31日

特許長官  
Commissioner,  
Patent Office

伴佐山建志



出証番号 出証特平10-3060513

【書類名】 特許願  
【整理番号】 NTT095201  
【提出日】 平成 9年 6月30日  
【あて先】 特許庁長官殿  
【国際特許分類】 G09C 1/00  
【発明の名称】 暗号装置  
【請求項の数】 8  
【発明者】  
【住所又は居所】 東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内  
【氏名】 神田 雅透  
【発明者】  
【住所又は居所】 東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内  
【氏名】 高嶋 洋一  
【発明者】  
【住所又は居所】 東京都武藏野市吉祥寺本町一丁目14番5号 エヌ・ティ・エイ・エレクトロニクスティクノロジー株式会社内  
【氏名】 青木 克彦  
【発明者】  
【住所又は居所】 神奈川県相模原市上鶴間2603-1-210  
【氏名】 松本 勉  
【特許出願人】  
【識別番号】 000004226  
【氏名又は名称】 日本電信電話株式会社  
【代表者】 宮津 純一郎  
【特許出願人】  
【識別番号】 591230295  
【氏名又は名称】 エヌ・ティ・エイ・エレクトロニクスティクノロジー株式

会社

【代表者】 鈴木 敏正

【代理人】

【識別番号】 100066153

【弁理士】

【氏名又は名称】 草野 卓

【手数料の表示】

【予納台帳番号】 002897

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9701407

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号装置

【特許請求の範囲】

【請求項 1】 入力データを初期分割手段で二つの部分データに分割し、これら部分データの一つに対し、非線形関数手段で鍵記憶手段に蓄積された鍵データに依存したデータ変換処理を行い、その非線形関数手段の出力データを前記部分データの他方の一つに線形演算手段で作用させ、その線形演算手段の出力データと前記非線形関数手段の入力部分データとの配列順番を交換手段で交換し、前記交換手段よりこの交換されたデータを二つの部分データとして前記非線形関数手段と、前記線形演算手段と前記交換手段とを繰返し手段で複数回繰返し、前記繰返し手段の最終回の繰返しにおける前記交換手段よりの二つのデータを一つの出力データに最終結合手段で結合して、その出力データを出力する暗号装置において、

前記非線形関数手段は、入力されたデータに前記鍵記憶手段に蓄積された鍵データに基づいて線形変換を行う鍵依存線形変換手段と、

その鍵依存線形手段の出力データを複数個のビット列に分割する分割手段と、

これらビット列にそれぞれ非線形変換を行う第一の非線形変換手段と、

前記第一の非線形変換手段のそれぞれの出力ビット列間で線形変換を行う第一の線形変換手段と、

その第一の線形変換手段の出力ビット列の少くとも一部に非線形変換を行う第二の非線形変換手段と、

その第二の非線形変換手段の出力ビット列を結合して前記非線形関数手段の出力データとする結合手段とを備えることを特徴とする暗号装置。

【請求項 2】 請求項 1 に記載の暗号装置において、

前記結合手段の出力データを線形変換して前記非線形関数手段の出力データとする第二の線形変換手段を備えることを特徴とする暗号装置。

【請求項 3】 請求項 1 または請求項 2 に記載の暗号装置において、

前記第一の線形変換手段は、前記鍵記憶手段に蓄積された鍵データに基づいて線形変換を行う手段であることを特徴とする暗号装置。

【請求項 4】 請求項 2 に記載の暗号装置において、

前記第二の線形変換手段は、前記鍵記憶手段に蓄積された鍵データに基づいて線形変換を行う手段であることを特徴とする暗号装置。

【請求項 5】 請求項 1 から請求項 4 までのいずれかに記載の暗号装置において、

前記入力データに線形変換を行って前記初期分割手段へ供給する初期線形変換手段を備えることを特徴とする暗号装置。

【請求項 6】 請求項 1 から請求項 5 までのいずれかに記載の暗号装置において、

前記最終結合手段の出力データに線形変換を行って暗号装置の出力とする最終線形変換手段を備えることを特徴とする暗号装置。

【請求項 7】 請求項 5 または請求項 6 に記載の暗号装置において、

前記初期線形変換手段は前記鍵記憶手段に蓄積された鍵データに基づいて線形変換を行う手段であることを特徴とする暗号装置。

【請求項 8】 請求項 6 に記載の暗号装置において、

前記最終線形変換手段は前記鍵記憶手段に蓄積された鍵データに基づいて線形変換を行う手段であることを特徴とする暗号装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、データの通信または蓄積において、データを秘匿するための暗号化装置、特に、秘密鍵の制御のもとでデータをブロック単位で暗号化または復号を行う共通鍵暗号方式による暗号化装置に関するものである。

【0002】

【従来の技術】

データを秘匿するための暗号化装置に含まれる代表的な共通鍵暗号方式には、米国連邦標準暗号である D E S (Data Encryption Standard) 暗号がある。

図 8 は、D E S 暗号の機能構成を示す。D E S 暗号では、56 ビットの秘密鍵を用い、64 ビットのデータブロック単位に暗号化または復号を行う。図 8 にお

いて、暗号化処理は、平文  $P$  の 64 ビットを初期変換部 1 1 において初期転値で変換した後、32 ビットごとのブロックデータ  $L_0, R_0$  に分割される。次に、 $R_0$  は図 9 に示す関数演算部 1 2 への入力として用いられ、関数演算部 1 2 において 48 ビットの拡大鍵  $k_0$  の制御のもとに  $f(R_0, k_0)$  に変換される。この変換データ  $f(R_0, k_0)$  と  $L_0$  との排他的論理和を回路 1 3 でとり、さらにその値と  $R_0$  とを入れ替えて、次のブロックデータ  $L_1, R_1$  を生成する。すなわち、 $R_1 = L_0 (+) f(R_0, k_0)$ ,  $L_1 = R_0$  である。このように二つのブロックデータ  $L_0, R_0$  を入力として演算部 1 2 と排他的論理和回路 1 3 とデータの入れ替えとにより  $L_1, R_1$  を出力する処理段 1 4<sub>0</sub> が構成され、同じような処理段 1 4<sub>1</sub> ~ 1 4<sub>15</sub> が継続的に設けられる。つまり各処理段 1 4<sub>i</sub> ( $0 \leq i < 16$ ) では、 $R_{i+1} = L_i (+) f(R_i, k_i)$ ,  $L_{i+1} = R_i$  の処理が行われ、最後に  $R_{16}, L_{16}$  を統合して 64 ビットにした後、最終転値部 1 5 において最終転値で変換して暗号文 64 ビットを出力する。復号処理においては、関数  $f$  に入力する拡大鍵  $k_0, k_1, \dots, k_{14}, k_{15}$  の順序だけを逆転させて、 $k_{15}, k_{14}, \dots, k_1, k_0$  の順に入力するようとする点を除けば、暗号化処理と同じ手順で実行できる。なお、拡大鍵  $k_0, k_1, \dots, k_{14}, k_{15}$  は、暗号化処理とは別の拡大鍵生成ルーチン 1 6 で 56 ビットの秘密鍵が 48 ビットの拡大鍵 16 個の計 768 ビットに拡大されることによって生成される。

## 【0003】

さて、関数演算内部 1 2 の処理は、図 9 に示すように行われる。まず、32 ビットのブロックデータ  $R_i$  は拡大転値部 1 7 で 48 ビットデータ  $E(R_i)$  に変換される。これに拡大鍵  $k_i$  とで排他的論理和を回路 1 8 で取り、48 ビットデータ  $E(R_i) (+) k_i$  に変換した後、8 個の 6 ビットごとのサブブロックデータに分割する。この 8 個のサブブロックデータはそれぞれ異なる  $S - b o x S_j$  ( $j = 0, 1, \dots, 7$ ) に入力され、各々が 4 ビットの出力を得る。なお、この  $S - b o x S_j$  は 6 ビットの入力データから 4 ビットの出力データに変換する非線形変換テーブルであり、DES 暗号の本質的な安全性を担っている部分である。 $S - b o x S_0 \sim S_7$  の 8 つの出力データは、再び連結されて 32 ビットデータになった後、転置変換部 1 9 を経て、図 8 に示されるように、 $L_i$  と

排他的論理和される関数  $f$  の出力  $f(R_i, k_i)$  となる。

#### 【0004】

次に、暗号解読法について述べる。DES暗号を始めとする従来の共通鍵暗号方式についてはさまざまな方面から暗号解読が試みられており、そのなかでも、極めて効果的な解読法であるのがE. Biham およびA. Shamirによって提案された差分解読法（“Differential Cryptanalysis of DES-like Cryptosystems.” Proceedings of CRYPTO' 90）と松井によって提案された線形解読法（“DES暗号の線形解読法（I）,” 1993年暗号と情報セキュリティシンポジウム SCIS'93-3C）である。

#### 【0005】

差分解読法は、2つのデータ  $X, X^*$  の差分を  $\Delta X = X (+) X^*$  としたとき、解読者が入手している平文・暗号文の2組を以下の式に適用して、最終ラウンドにおける拡大鍵  $k_{15}$  を求めることを目的としている。

$$f(L_{16}, k_{15}) (+) f((L_{16} (+) \Delta L_{16}), k_{15}) = \Delta R_{16} (+) \Delta R_{14}$$

このとき、 $L_{16}, \Delta L_{16}, \Delta R_{16}$  は暗号文から得られるデータであるので既知の情報である。このため、解読者が  $\Delta R_{14}$  を正しく求めることができるならば、上式は  $k_{15}$  のみが未知定数となり、既知の平文・暗号文の組を用いて  $k_{15}$  に関する全数探索を行うことで、解読者は必ず正しい  $k_{15}$  を見つけだすことができる。一方、 $\Delta R_{14}$  についてみてみると、この値は中間差分値であるため、一般には求めることが困難である。そこで、1ラウンド目から最終ラウンドの一つ前までのラウンド目までにおいて、各ラウンドが確率  $p_i$  で  $\Delta R_{i+1} = \Delta L_i (+) \{f(\Delta R_i)\}$ ,  $\Delta L_{i+1} = \Delta R_{i+1}$  のように近似されるとおく。ここでのポイントは、ある  $\Delta R_i$  が入力されたとき、拡大鍵  $k_i$  の値に関わらず、確率  $p_i$  で  $\{f(\Delta R_i)\}$  を予測できるということにある。このように近似できるのは、 $\{f(\Delta R_i)\}$  に影響を与えるのが非線形な変換である  $S - box$  の部分だけであり、しかも  $S - box$  において、入力差分によっては差分出力の分布に極めて大きな偏りが生じるためである。例えば、 $S1 - box$  では、入力差分「10100」のとき、 $1/4$  の確率で出力差分「0010」に変換されるためである。そこで、各々の  $S - box$  が確率  $p_{si}$  で入力差分と出力差分との関係が予

測できるとおき、これらを組み合わせることで各ラウンドの近似を求める。さらに、各ラウンドでの近似を連結していくことで、 $\Delta R_{14}$  は確率  $P = \prod p_i$  で  $\Delta L_0$ ,  $\Delta R_0$  ( $\Delta L_0$ ,  $\Delta R_0$  は平文から得られるデータであるので既知の情報である) から求められることになる。なお、この確率  $P$  が大きいほど、暗号解読が容易である。このようにして、拡大鍵  $k_{15}$  が求められると、今度は 1 段少ない 1 5 段 DES 暗号とみなして、同様の手法で、拡大鍵  $k_{14}$  を求めていくということを繰り返して、最終的に拡大鍵  $k_0$  まで求めていく。

## 【0006】

Biham らによると、この解読法では、 $2^{47}$  組の選択された既知平文・暗号文の組があれば DES 暗号を解読できるとしている。

また、線形解読法は、以下の線形近似式を構成し、解読者が入手している平文・暗号文の組による最尤法を用いて拡大鍵を求める目的としている。

$$(L_0, R_0) \cdot \Gamma(L_0, R_0) (+) (L_{16}, R_{16}) \cdot \Gamma(L_{16}, R_{16}) = (k_0, k_1, \dots, k_{15}) \cdot \Gamma(k_0, k_1, \dots, k_{15})$$

ただし、 $\Gamma(X)$  は  $X$  の特定のビット位置を選択するベクトルを表し、マスク値という

線形近似式の役割は、暗号アルゴリズム内部を線形表現で近似的に置き換え、平文・暗号文の組に関する部分と拡大鍵に関する部分とに分離することにある。つまり、平文・暗号文の組に関して、平文の特定のビット位置の値と暗号文の特定のビット位置の値との全ての排他的論理和が一定値となり、その値は拡大鍵の特定のビット位置の値の排他的論理和に等しくなることを表している。したがって、解読者は  $(L_0, R_0) \cdot \Gamma(L_0, R_0) (+) (L_{16}, R_{16}) \cdot \Gamma(L_{16}, R_{16})$  の情報から  $(k_0, k_1, \dots, k_{15}) \cdot \Gamma(k_0, k_1, \dots, k_{15})$  (1 ビット) の情報が得られるということになる。このとき、 $(L_0, R_0)$ ,  $(L_{16}, R_{16})$  はそれぞれ平文・暗号文のデータであるので既知の情報である。このため、解読者が  $\Gamma(L_0, R_0)$ ,  $\Gamma(L_{16}, R_{16})$ ,  $\Gamma(k_0, k_1, \dots, k_{15})$  を正しく求めることができるならば、 $(k_0, k_1, \dots, k_{15}) \cdot \Gamma(k_0, k_1, \dots, k_{15})$  (1 ビット) を求めることができる。

## 【0007】

DES暗号では、非線形な変換が起きる部分は  $S - b \circ x$  しかないので、 $S - b \circ x$  についてのみ線形表現ができれば、容易に線形近似式が構成できる。そこで、各々の  $S - b \circ x$  が確率  $p_{si}$  で線形表現できるとおく。ここでのポイントは、 $S - b \circ x$  に対する入力マスク値が与えられたとき、確率  $p_{si}$  でその出力マスク値を予測できるということである。これは、非線形変換テーブルである  $S - b \circ x$  において、入力マスク値によっては差分マスク値の分布に極めて大きな偏りが生じるためにおこる。例えば、 $S5 - b \circ x$  では、入力マスク値「010000」のとき、 $3/16$  の確率で出力マスク値「1111」が予測されるためである。これら  $S - b \circ x$  におけるマスク値を組み合わせることによって、各ラウンドが確率  $p_i$  で入力マスク値と出力マスク値のあいだに線形近似することができ、各ラウンドでの線形近似を連結していくことで、 $\Gamma(L_0, R_0)$ ,  $\Gamma(L_{16}, R_{16})$ ,  $\Gamma(k_0, k_1, \dots, k_{15})$  は確率  $P = 2^{n-1} \cdot \prod |p_i - 1/2|$  で求められることになる。なお、この確率  $P$  が大きいほど、暗号解読が容易である。

#### 【0008】

松井によると、この解読法で、 $2^{43}$ 組の既知平文・暗号文の組を用いて、DES暗号の解読に成功している。

さて、上記の解読法に対抗するためには、確率  $P$  が十分に小さくなければよい。このため、確率  $P$  を小さくするための提案がさまざま行われており、なかでも従来の暗号方式において、もっとも簡単に安全性を高めるための方法がラウンド数を増やすことであった。例えば、DES暗号を3つつなげたTriple-DES暗号は、実質的にDESのラウンド数を16段から48段に増やした暗号方式であり、確率  $P$  は、DES暗号よりもはるかに小さい。

#### 【0009】

##### 【発明が解決しようとする課題】

しかし、上記の解読法に対抗するための対策として、ラウンド数を増加させることは、暗号化速度を犠牲にすることになる。例えば、ラウンド数を3倍に増やせば、暗号化速度は  $1/3$  になる。つまり、現在のDES暗号の暗号化速度はPentium PCクラスで約  $10 \text{ M b p s}$  であるため、Triple-DES暗号ともなると約  $3.5 \text{ M b p s}$  まで暗号化速度が低下する。一方で、ネットワークやコンピュ

ータなどは年々高速化しており、暗号化装置もそれらの高速化に対応したものが望まれている。

【0010】

このため、従来の暗号装置では、それらの高速化の要求に対して、安全性と高速性を同時に満たすことはきわめて困難な状況になっている。

この発明の目的は、上記の点を鑑みなされたもので、関数  $f$  を安全性と高速性を同時に満たすような構造にすることによって、ラウンド数を増加させることなく安全性を確保し、かつ高速な暗号化処理が可能となるような暗号装置を提供することにある。

【0011】

【課題を解決するための手段】

この発明では、特に非線形関数手段において、非線形関数手段の入力データに鍵記憶手段に蓄積された鍵データに基づいて線形変換を行う鍵依存線形変換手段と、この鍵依存線形変換手段の出力データを複数個のビット列に分割する分割手段と、これら分割された各ビット列に非線形変換をそれぞれ行う第一の非線形変換手段と、その第一の非線形変換手段の各々の出力ビット列間で線形変換を行う第一の線形変換手段と、その第一の線形変換手段の出力ビット列の一部またはすべてに非線形変換を行う第二の非線形変換手段と、その第二の非線形変換手段の出力ビット列をその非線形関数手段の出力データに結合する結合手段とを備えることを特徴とする。

【0012】

さらに安全性を向上させるには、前記結合手段の出力データを前記非線形関数手段の出力データに線形変換を行う第二の線形変換手段を備えることを特徴とする。

また、前記第一の線形変換手段または前記第二の線形変換手段、もしくはその両方の手段が、データの線形変換を行うときに、前記鍵記憶手段に蓄積された鍵データに基づいて線形変換を行う鍵依存線形変換手段であることを特徴とする。

作用

この発明によれば、 $S - b \circ x$ における確率が  $p_{si} \leq p_b < 1$  であるとき ( $p$

$b$  は  $S - b \circ x$  の最大確率)、各ラウンドを近似するときの確率は  $p_i \leq p_b^2$  (ただし、差分解読法の場合は関数  $f$  への入力差分が 0 でないとき、線形解読法の場合は関数  $f$  での出力マスク値が 0 でないとき) となることが保証される。また、関数  $f$  が全単射 (入力が異なれば出力が必ず異なる) であるとき、暗号方式のラウンド数を  $3m$  とすると、暗号方式としての確率は  $P \leq p_i^{2m} \leq p_b^{4m}$  となる。一般に、暗号方式では  $P < 2^{-64}$  であれば差分解読法や線形解読法に対して安全とされるため、 $m > -16 / (\log_2(p_b))$  を満たせばよく、 $p_b \leq 2^{-4}$  であれば DES 暗号の 16 ラウンドよりも少ないラウンド数で安全性を確保できる。なお安全性の確率は  $m$  ラウンドの倍数ごとに変化する。

## 【0013】

また、少なくとも 2 つの  $S - b \circ x$  が並列に処理できるような配置となっているため、並列処理ができないものと比較して 2 倍以上の処理速度を出すことが可能である。

ゆえに、差分解読法や線形解読法に対する安全性を、高速な関数で、かつ比較的少ないラウンド数で確保できるため、安全性と高速性を両立させた暗号装置を提供することが可能になる。

## 【0014】

## 【発明の実施の形態】

実施例 1

以下、この発明の一実施例を図面を用いて説明する。

図 1 は、この発明の一実施例を示す暗号装置における、暗号化処理手順の機能構成を示したものである。

## 【0015】

平文に相当する入力データ  $P$  を入力手段 301 から暗号装置内に入力する。入力データ  $P$  は鍵記憶手段 322 に蓄積されている鍵データ  $f_k$  による鍵依存初期線形変換手段 302 で変換された後、初期分割手段 303 で二つのデータ  $L_0$ ,  $R_0$  に分割される。例えば 64 ビットのデータが 32 ビットづつのデータ  $L_0$ ,  $R_0$  にビット分割される。データ  $R_0$  は、鍵記憶手段 322 に蓄積されている鍵データ  $k_{00}$ ,  $k_{10}$ ,  $k_{20}$  とともに非線形関数手段 304 に入力され、非線形関数

手段304で変換処理を行われてデータ $Y_0$ に変換される。データ $Y_0$ とデータ $L_0$ は線形演算手段305で演算されてデータ $L_0^*$ に変換される。データ $L_0^*$ とデータ $R_0$ は交換手段306でデータ位置の交換が行われ、 $L_1 = R_0$ ,  $R_1 = L_0^*$ のように交換される。以下、二つのデータ $L_1$ ,  $R_1$ について上記と同様の処理を繰り返し行う。すなわち、二つのデータ $L_i$ ,  $R_i$ について、データ $R_i$ は、鍵記憶手段322に蓄積されている鍵データ $k_{0i}$ ,  $k_{1i}$ ,  $k_{2i}$ とともに非線形関数手段304に入力され、非線形関数手段304で変換処理を行われて、データ $Y_i$ に変換される。データ $Y_i$ とデータ $L_i$ は線形演算手段305で演算されてデータ $L_i^*$ に変換される。データ $L_i^*$ とデータ $R_i$ は交換手段306でデータ位置の交換が行われ、 $L_{i+1} = R_i$ ,  $R_{i+1} = L_i^*$ のように交換される。線形演算手段305は例えば排他的論理和演算を行うものである。

## 【0016】

暗号方式としての安全性を確保するための適切な繰り返し回数を $n$ とすると、繰り返し処理の結果、データ $L_n$ ,  $R_n$ が得られる。このデータ $L_n$ ,  $R_n$ を最終結合手段307で結合しつまり例えば32ビットの各 $L_n$ ,  $R_n$ をビット結合して64ビットのデータとし、その後鍵記憶手段322に蓄積されている鍵データ $e_k$ による鍵依存最終線形変換手段308で変換し、出力手段309から暗号文として出力データ $C$ を出力する。

## 【0017】

復号については、暗号化処理手順と逆の手順をたどることによって、暗号文 $C$ から平文 $P$ が得られる。例えば図1において入力データの代りに暗号文データを入力し、鍵データを図1とは逆に、 $e_k$ ,  $k_{0(n-1)}$ ,  $k_{1(n-1)}$ ,  $k_{2(n-1)}$ ,  $\dots$ ,  $k_{01}$ ,  $k_{11}$ ,  $k_{21}$ ,  $k_{00}$ ,  $k_{10}$ ,  $k_{20}$ ,  $f_k$ を順次与えればよい。

次に、非線形関数手段304の内部を詳細に説明する。図2は、非線形関数手段304の内部の機能構成を抜き出して示したものである。

## 【0018】

データ $R_i$ は、鍵記憶手段322に蓄積されている鍵データ $k_{0i}$ ,  $k_{1i}$ ,  $k_{2i}$ とともに非線形関数手段304への入力データとなる。データ $R_i$ は、鍵データ $k_{0i}$ による鍵依存線形変換手段341によりデータ $R_i^*$ に線形変換される。次

に、データ  $R_i^*$  は分割手段 342において例えれば8ビットづつの4つのデータ  $in_0, in_1, in_2, in_3$  にビット分割される。4つのデータ  $in_0, in_1, in_2, in_3$  は、それぞれ非線形変換手段 343, 344, 345, 346において、データ  $mid_{00}, mid_{01}, mid_{02}, mid_{03}$  に非線形変換された後、鍵依存線形変換手段 347に入力される。鍵依存線形変換手段 347では、鍵データ  $k_{1i}$  により例えば図3に示すように、線形処理される。即ちデータ  $mid_{00}, mid_{01}, mid_{02}, mid_{03}$  はそれぞれ処理系  $30_0 \sim 30_3$  に入力され、処理系  $30_1$  で  $mid_{00}$  と  $mid_{01}$  との排他的論理和が回路  $31_1$  でとられ、また処理系  $30_2$  で  $mid_{02}$  と  $mid_{03}$  の排他的論理和が回路  $31_2$  でとられ、更に回路  $31_1$  の出力と回路  $31_2$  の出力の排他的論理和が回路  $32_2$  でとられる。回路  $31_1$  の出力と回路  $32_2$  の出力との排他的論理和が回路  $31_1$  でとられ、回路  $33_1$  の出力と  $mid_{00}$  の排他的論理和が回路  $34_0$  でとられ、回路  $32_2$  の出力と  $mid_{03}$  との排他的論理和が回路  $34_3$  でとられ、回路  $34_0, 33_1, 32_2, 34_3$  の各出力と鍵データ  $k_{1i0}, k_{1i1}, k_{1i2}, k_{1i3}$  との各排他的論理和が回路  $35_0 \sim 35_3$  でそれぞれとられて、それぞれ  $mid_{10}, mid_{11}, mid_{12}, mid_{13}$  を出力する。つまりデータ  $mid_{00}, mid_{01}, mid_{02}, mid_{03}$  は相互に関連づけられた後、それぞれ鍵データ  $k_{1i0}, k_{1i1}, k_{1i2}, k_{1i3}$  に依存した線形変換が行われる。論理式で示すと下記の論理演算がなされる。

【0019】

$$\begin{aligned}
 mid_{10} &= mid_{00} (+) mid_{02} (+) mid_{03} (+) k_{1i0}, mid_{11} = mid_{02} (+) mid_{03} (+) k_{1i1}, \\
 mid_{12} &= mid_{00} (+) mid_{01} (+) mid_{02} (+) mid_{03} (+) k_{1i2}, mid_{13} = mid_{00} (+) mid_{01} (+) mid_{02} (+) k_{1i3}
 \end{aligned}$$

次にこれらデータ  $mid_{10}, mid_{11}, mid_{12}, mid_{13}$  は、それぞれ非線形変換手段 348, 349, 350, 351において、データ  $out_0, out_1, out_2, out_3$  に非線形変換された後、結合手段 352において、一つのデータ  $Y_i^*$  に結合される。つまり例えば4つの8ビットのデータが1つの32ビットデータにビット結合される。最後に、データ  $Y_i^*$  は、鍵データ  $k_{2i}$  による鍵依存線形変換手段 353において、データ  $Y_i$  に線形変換され、非線形関

数手段 304 からの出力データ  $Y_i$  が生成される。非線形変換手段 343～346, 348～351 の各 1 つの手段それぞれ、例えば DES 暗号の S-box の 1 つの要素のようなもので、それぞれ入力データに応じた異った出力データを出力するものである。

## 【0020】

ここで、非線形変換手段 343～346 は 4 つ並列に配置されており、その変換処理は相互に関連していないため、これらは並列実行が可能である。また、非線形変換手段 348～351 についても同様のことがいえる。

さらに、非線形変換手段 348～351 については、鍵依存線形変換手段 347 が任意の鍵依存線形変換方法をとることを可能にするために配置されている。このため、鍵依存線形変換手段 347 が、例えば図 3 のように特定の線形変換であることがあらかじめわかっている場合には、非線形変換手段 348～351 の一部を削除しても、差分解読法および線形解読法に対する安全性が低下しないようにすることができ、削除した分だけ暗号化処理速度の向上が望める。例えば、鍵依存線形変換手段 347 が図 3 で表されているとき、非線形変換手段 349, 350 を削除しても差分解読法および線形解読法に対する安全性は低下しない一方で、暗号化速度が約 33% 向上する。つまり鍵依存線形変換手段 347 が予め決っている場合は差分解読法、線形解読法に対しては非線形変換手段 348～351 の一部はその存在が安全性に関係ない場合があり、その部分は省略できる。

なお、鍵データ  $f_k, k_{00}, k_{10}, k_{20}, k_{01}, k_{11}, k_{21}, \dots, k_{0(n-1)}, k_{1(n-1)}, k_{2(n-1)}, e_k$  は図 1 において鍵入力手段 320 から暗号装置内に入力された鍵情報 Key から鍵データ生成手段 321 によって変換され、鍵記憶手段 322 に蓄積されたデータである。鍵データ生成手段 321 による鍵データの生成は DES 暗号の拡大鍵生成アルゴリズム 16 と同様に行うことができる。

## 【0021】

上記のように構成された暗号装置の場合、例えば、非線形変換手段 343～346, 348～351 の各 1 つづつが差分解読法および線形解読法に対して確率  $p_b = 2^{-6}$  で近似表現できるように設計されているならば、各ラウンドは非線形

変換を必ず2回行うため、確率  $p_i \leq 2^{-12}$  で近似表現することができ、暗号装置全体としてはラウンド数を  $3m$  として、確率  $P \leq 2^{-24m}$  で近似表現できることになる。ここで、例えば  $m=4$  (ラウンド数12段) とすると、 $P \leq 2^{-96}$  となり、差分解読法および線形解読法に対して十分安全な暗号装置となる。

### 【0022】

また、鍵依存初期線形変換手段302、鍵依存最終線形変換手段308、鍵依存線形変換手段347、353は鍵に依存する線形変換手段であるため、差分解読法および線形解読法以外の解読法に対しても十分な安全性を兼ね備え、もっとも安全性を重視した暗号装置である。

なお、この発明はこの例に特定されるだけでなく、例えば高速性を望むのであれば、これら鍵依存初期線形変換手段302、鍵依存最終線形変換手段308、鍵依存線形変換手段353については、そのいずれか、もしくはすべてを削除することが可能である。この場合、差分解読法および線形解読法に対する安全性は低下しない一方で、削除した分だけ暗号化処理速度の向上が望める。ただし他の解読法に対しては弱くなるおそれはある。また、鍵依存初期線形変換手段302、鍵依存最終線形変換手段308、鍵依存線形変換手段347、353のいずれか、もしくはすべてを鍵に依存しない線形変換手段に変更することも可能である。この場合、差分解読法および線形解読法以外の解読法に対しても安全性が低下しない一方で、インプリメントを最適化することにより、暗号化処理速度の向上が望める。なお、線形変換手段としては、ビット位置を予め決めた関係で入れかえる転置、予め決めたビット数だけ回転シフトするなどを行う。鍵依存線形変換手段は、鍵データに応じたビット数だけ回転シフトする、あるいは、鍵データとの排他的論理和演算を行うものなどである。

### 実施例2

図4は、この発明の他の実施例を示す。

### 【0023】

平文に相当する入力データPを入力手段301から暗号装置内に入力する。入力データPは初期分割手段303で二つのデータ  $L_0, R_0$  に分割される。データ  $R_0$  は、鍵記憶手段322に蓄積されている鍵データ  $k_{00}, k_{20}$  とともに非線

形関数手段304に入力され、非線形関数手段304で変換処理を行われて、データ $Y_0$ に変換される。データ $Y_0$ とデータ $L_0$ は線形演算手段305で演算され、データ $L_0^*$ に変換される。データ $L_0^*$ とデータ $R_0$ は交換手段306でデータ位置の交換が行われ、 $L_1 = R_0$ ,  $R_1 = L_0^*$ のように交換される。以下、二つのデータ $L_1$ ,  $R_1$ について上記と同様の処理を繰り返し行う。すなわち、二つのデータ $L_i$ ,  $R_i$ について、データ $R_i$ は、鍵記憶手段322に蓄積されている鍵データ $k_{0i}$ ,  $k_{2i}$ とともに非線形関数手段304に入力され、非線形関数手段304で変換処理を行われて、データ $Y_i$ に変換される。データ $Y_i$ とデータ $L_i$ は線形演算手段305で演算され、データ $L_i^*$ に変換される。データ $L_i^*$ とデータ $R_i$ は交換手段306でデータ位置の交換が行われ、 $L_{i+1} = R_i$ ,  $R_{i+1} = L_i^*$ のように変換される。

## 【0024】

暗号方式としての安全性を確保するための適切な繰り返し回数を $n$ とすると、繰り返し処理の結果、データ $L_n$ ,  $R_n$ が得られる。このデータ $L_n$ ,  $R_n$ を最終結合手段307で結合した後、出力手段309から暗号文として出力データCを出力する。

復号については、暗号化処理手順と逆の手順をたどることによって、暗号文Cから平文Pが得られる。

## 【0025】

次に、非線形関数手段304の内部を詳細に説明する。図5Aは、非線形関数手段304の内部の機能構成を抜き出して示したものである。

データ $R_i$ は、鍵記憶手段322に蓄積されている鍵データ $k_{0i}$ ,  $k_{2i}$ とともに非線形関数手段304への入力データとなる。データ $R_i$ は、データ $k_{0i}$ による鍵依存線形変換341において、データ $R_i^*$ に線形変換される。次に、データ $R_i^*$ は分割手段342において4つのデータ $i_{n_0}$ ,  $i_{n_1}$ ,  $i_{n_2}$ ,  $i_{n_3}$ に分割される。4つのデータ $i_{n_0}$ ,  $i_{n_1}$ ,  $i_{n_2}$ ,  $i_{n_3}$ は、それぞれ非線形変換手段343, 344, 345, 346において、データ $mid_{00}$ ,  $mid_{01}$ ,  $mid_{02}$ ,  $mid_{03}$ に非線形変換された後、線形変換手段354に入力される。線形変換手段354では、例えば図5Bに示すように相互に関連づけるよ

うに変換される。これは図3中の鍵データとの論理演算を省略した場合と同一の例であり、下記の式で表わせる。

## 【0026】

$mid_{10} = mid_{00} (+) mid_{02} (+) mid_{03}$ ,  $mid_{11} = mid_{02} (+) mid_{03}$ ,

$mid_{12} = mid_{00} (+) mid_{01} (+) mid_{02} (+) mid_{03}$ ,  $mid_{13} = mid_{00} (+) mid_{01} (+) mid_{02}$

この線形変換で、データ  $mid_{10}$ ,  $mid_{11}$ ,  $mid_{12}$ ,  $mid_{13}$  が生成され、そのうちのデータ  $mid_{10}$ ,  $mid_{13}$  は、それぞれ非線形変換手段348, 351において、データ  $out_0$ ,  $out_3$  に非線形変換された後、結合手段352において、4つのデータ  $out_0$ ,  $mid_{11}$ ,  $mid_{12}$ ,  $out_3$  を一つのデータ  $Y_i^*$  に結合される。最後に、データ  $Y_i^*$  は、データ  $k_{2i}$  による鍵依存線形変換手段353において、データ  $Y_i$  に線形変換され、非線形関数手段304からの出力データ  $Y_i$  が生成される。

## 【0027】

ここで、非線形変換手段343～346は4つ並列に配置されており、その変換処理は相互に関連していないため、これらは並列実行が可能である。また、非線形変換手段348, 351についても同様のことがいえる。

なお、鍵データ  $k_i$  は、鍵入力手段320から暗号装置内に入力された鍵情報 Key から鍵データ生成手段321によって変換され、鍵記憶手段322に蓄積されたデータである。

## 【0028】

上記のように構成された暗号装置の場合、例えば、非線形変換手段343～346, 348, 351が差分解読法および線形解読法に対して確率  $p_b = 2^{-6}$  で近似表現できるように設計されているならば、実施例1と同様に各ラウンドは確率  $p_i \leq 2^{-12}$  で近似表現することができ、暗号装置全体としてはラウンド数を  $3m$  として、確率  $p \leq 2^{-24m}$  で近似表現できることになる。ここで、例えば  $m = 4$  (ラウンド数12段) とすると、 $P \leq 2^{-96}$  となり、差分解読法および線形解読法に対して十分安全な暗号装置となる。

## 【0029】

また、鍵依存線形変換手段353があるため、差分解読法と線形解読法以外の

解読法に対しても安全性にマージンがある構造であり、かつ実施例1よりも構造が簡素化されているため、高速である。つまり、安全性と高速性のバランスを重視した暗号装置である。

### 実施例3

図6は、この発明の更に他の実施例を示す。

#### 【0030】

平文に相当する入力データPを入力手段301から暗号装置内に入力する。入力データPは初期分割手段303で二つのデータ $L_0$ ,  $R_0$ に分割される。データ $R_0$ は、鍵記憶手段322に蓄積されている鍵データ $k_0$ とともに非線形関数手段304に入力され、非線形関数手段304で変換処理を行われて、データ $Y_0$ に変換される。データ $Y_0$ とデータ $L_0$ は線形演算手段305で演算され、データ $L_0^*$ に変換される。データ $L_0^*$ とデータ $R_0$ は交換手段306でデータ位置の交換が行われ、 $L_1 = R_0$ ,  $R_1 = L_0^*$ のように変換される。以下、二つのデータ $L_1$ ,  $R_1$ について上記と同様の処理を繰り返し行う。すなわち、二つのデータ $L_i$ ,  $R_i$ について、データ $R_i$ は、鍵記憶手段322に蓄積されている鍵データ $k_i$ とともに非線形関数手段304に入力され、非線形関数手段304で変換処理を行われて、データ $Y_i$ に変換される。データ $Y_i$ とデータ $L_i$ は線形演算手段305で演算され、データ $L_i^*$ に変換される。データ $L_i^*$ とデータ $R_i$ は交換手段306でデータ位置の交換が行われ、 $L_{i+1} = R_i$ ,  $R_{i+1} = L_i^*$ のように変換される。

#### 【0031】

暗号方式としての安全性を確保するための適切な繰り返し回数をnとすると、繰り返し処理の結果、データ $L_n$ ,  $R_n$ が得られる。このデータ $L_n$ ,  $R_n$ を最終結合手段307で結合した後、出力手段309から暗号文として出力データCを出力する。

復号については、暗号化処理手順と逆の手順をたどることによって、暗号文Cから平文Pが得られる。

#### 【0032】

次に、非線形関数手段304の内部を詳細に説明する。図7は、非線形関数手

段304の機能構成を抜き出して示したものである。

非線形関数手段304への入力データ $R_i$ は、鍵記憶手段322に蓄積されている鍵データ $k_i$ とともに鍵依存線形変換341への入力となる。データ $R_i$ は、データ $k_i$ による鍵依存線形変換341において、データ $R_i^*$ に線形変換される。次に、データ $R_i^*$ は分割手段342において4つのデータ $i n_0, i n_1, i n_2, i n_3$ に分割される。4つのデータ $i n_0, i n_1, i n_2, i n_3$ は、それぞれ非線形変換手段343, 344, 345, 346において、データ $mid_{00}, mid_{01}, mid_{02}, mid_{03}$ に非線形変換された後、線形変換手段354に入力される。線形変換手段354では、例えば実施例2の図5Bと同じように、

$$mid_{10} = mid_{00} (+) mid_{02} (+) mid_{03}, mid_{11} = mid_{02} (+) mid_{03},$$

$$mid_{12} = mid_{00} (+) mid_{01} (+) mid_{02} (+) mid_{03}, mid_{13} = mid_{00} (+) mid_{01} (+) mid_{02}$$

に線形変換し、データ $mid_{10}, mid_{11}, mid_{12}, mid_{13}$ を生成する。ついで、データ $mid_{10}, mid_{13}$ は、それぞれ非線形変換手段348, 351において、データ $out_0, out_3$ に非線形変換された後、結合手段352において、4つのデータ $out_0, mid_{11}, mid_{12}, out_3$ を一つのデータに結合され、非線形関数手段304からの出力データ $Y_i$ が生成される。

### 【0033】

ここで、非線形変換手段343～346は4つ並列に配置されており、その変換処理は相互に関連していないため、これらは並列実行が可能である。また、非線形変換手段348, 351についても同様のことがいえる。

なお、鍵データ $k_i$ は、鍵入力手段320から暗号装置内に入力された鍵情報Keyから鍵データ生成手段321によって変換され、鍵記憶手段322に蓄積されたデータである。

### 【0034】

上記のように構成された暗号装置の場合、例えば、非線形変換手段343～346, 348, 351が差分解読法および線形解読法に対して確率 $p_b = 2^{-6}$ で近似表現できるように設計されているならば、各ラウンドは確率 $p_i \leq 2^{-12}$ で近似表現することができ、暗号装置全体としてはラウンド数を3mとして、確率

$P \leq 2^{-24m}$  で近似表現できることになる。ここで、例えば  $m = 4$  (ラウンド数 1 2 段) とすると、 $P \leq 2^{-96}$  となり、差分解読法および線形解読法に対して十分安全な暗号装置となる。

【0035】

また、差分解読法および線形解読法に対して十分な安全性を確保するために最低限必要な手段しか実行しない構造であるため、もっとも高速性を重視した暗号装置である。

上述において、非線形関数手段 304 中の各分割手段 342 は 4 分割に限らず、複数に分割すればよい。なお、4 分割の場合においては、第二の非線形変換手段は図 5A、図 7 に示したように二つのみとすることができる。

【0036】

【発明の効果】

以上、詳細に説明したように、この発明によれば、非線形関数手段で入力データを複数に分割し、かつそれぞれ非線形変換を行い、その後、相互に線形交換を行い、更に少くとも一部を非線形交換することによりデータの通信または蓄積においてデータを秘匿するための暗号装置について、安全性が高く、かつ高速性を兼ね備えた暗号装置を提供することができる。

【図面の簡単な説明】

【図 1】

この発明の実施例 1 の機能構成を示す図。

【図 2】

実施例 1 における非線形関数手段 304 の詳細な機能構成例を示す図。

【図 3】

図 2 中の鍵依存線形変換手段 347 の具体例を示す図。

【図 4】

この発明の実施例 2 の機能構成を示す図。

【図 5】

A は実施例 2 における非線形関数手段 304 の詳細な機能構成を示す図、B はこの手段 304 中の具体例を示す図である。

【図 6】

この発明の実施例 3 の機能構成を示す図。

【図 7】

実施例 3 における非線形関数手段 304 の詳細な機能構成を示す図。

【図 8】

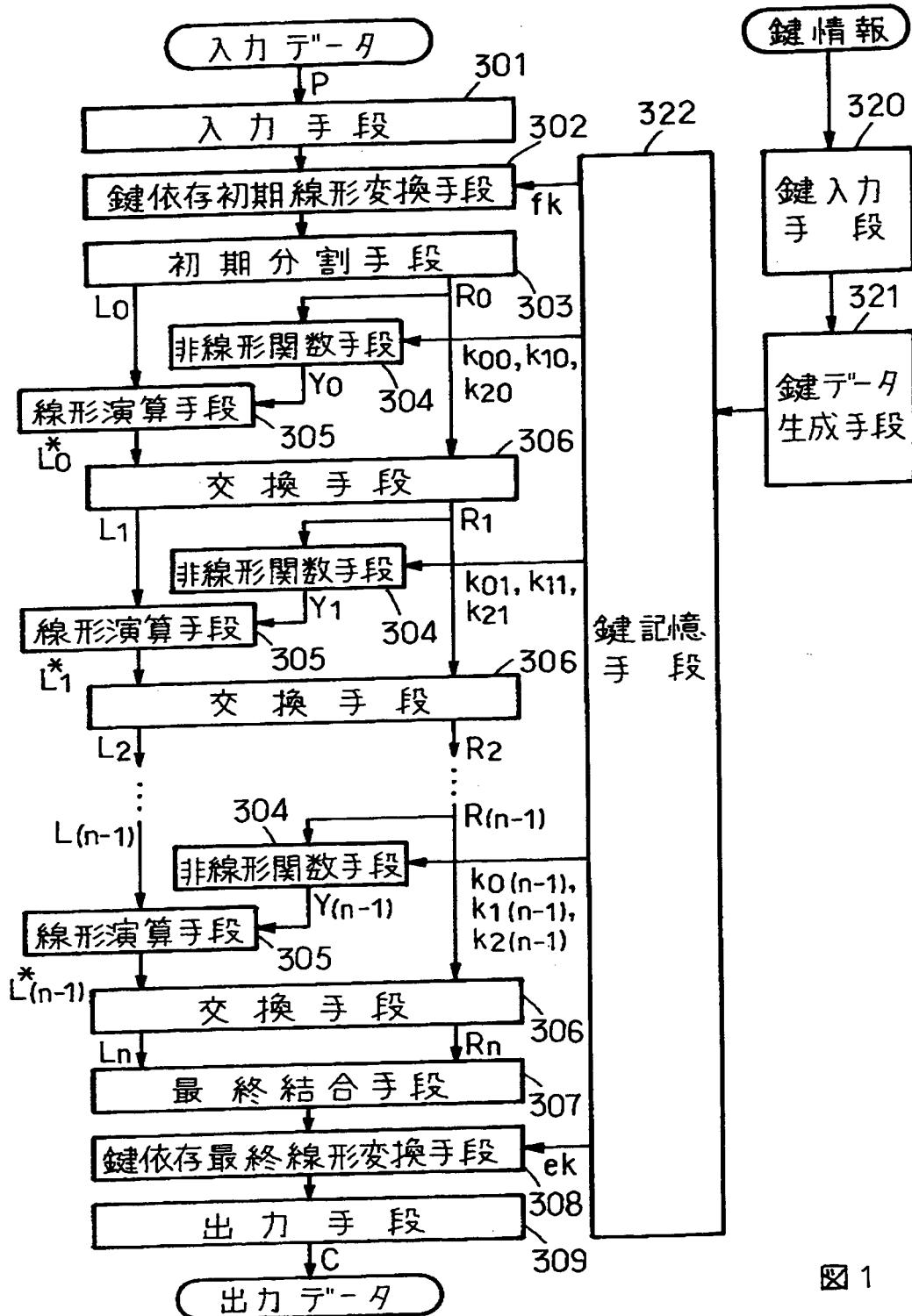
従来の D E S 暗号装置の機能構成を示す図。

【図 9】

図 8 中の f 関数演算部 12 の具体的機能構成を示す図。

【書類名】 図面

【図1】



1

【図2】

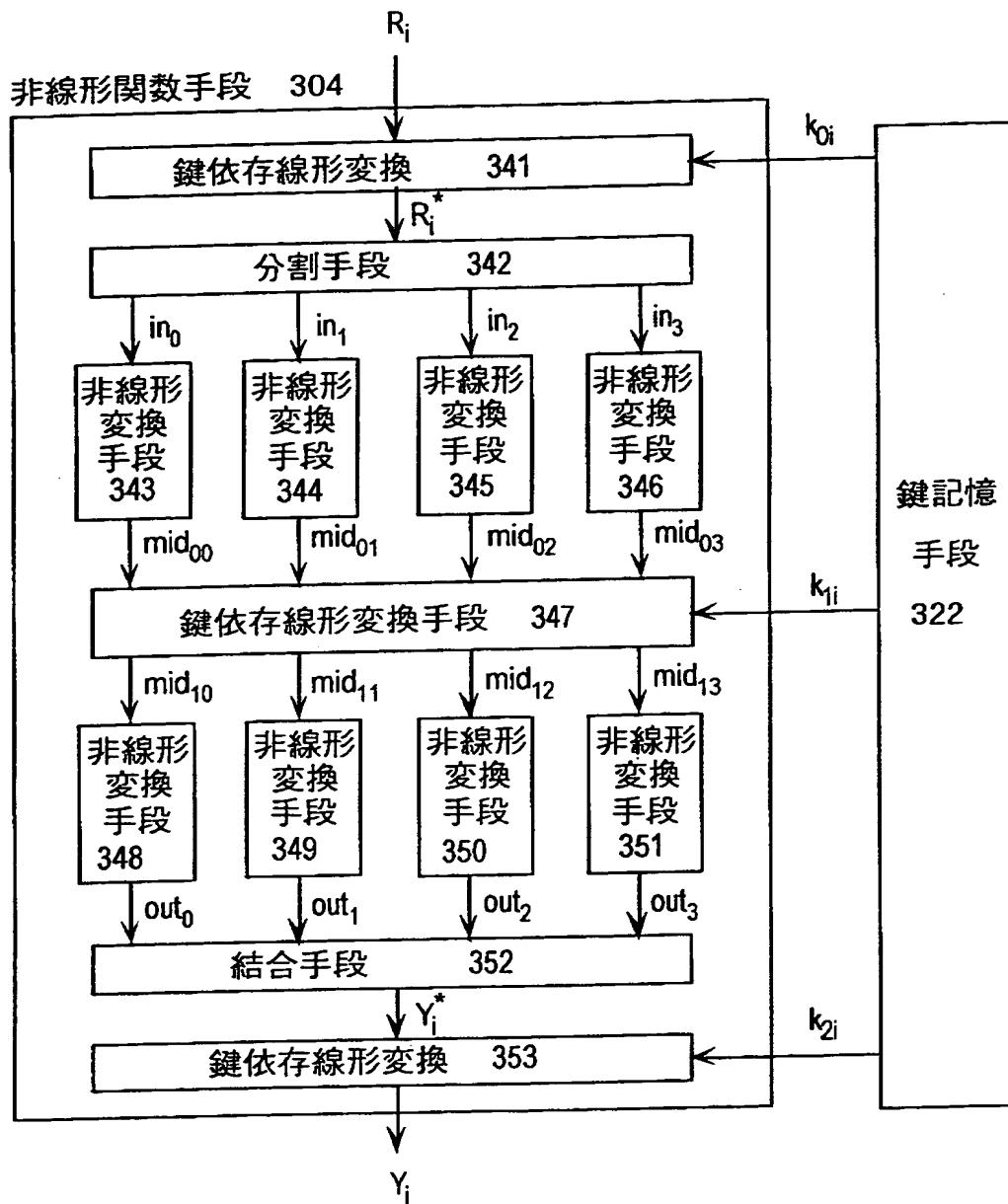


図2

【図3】

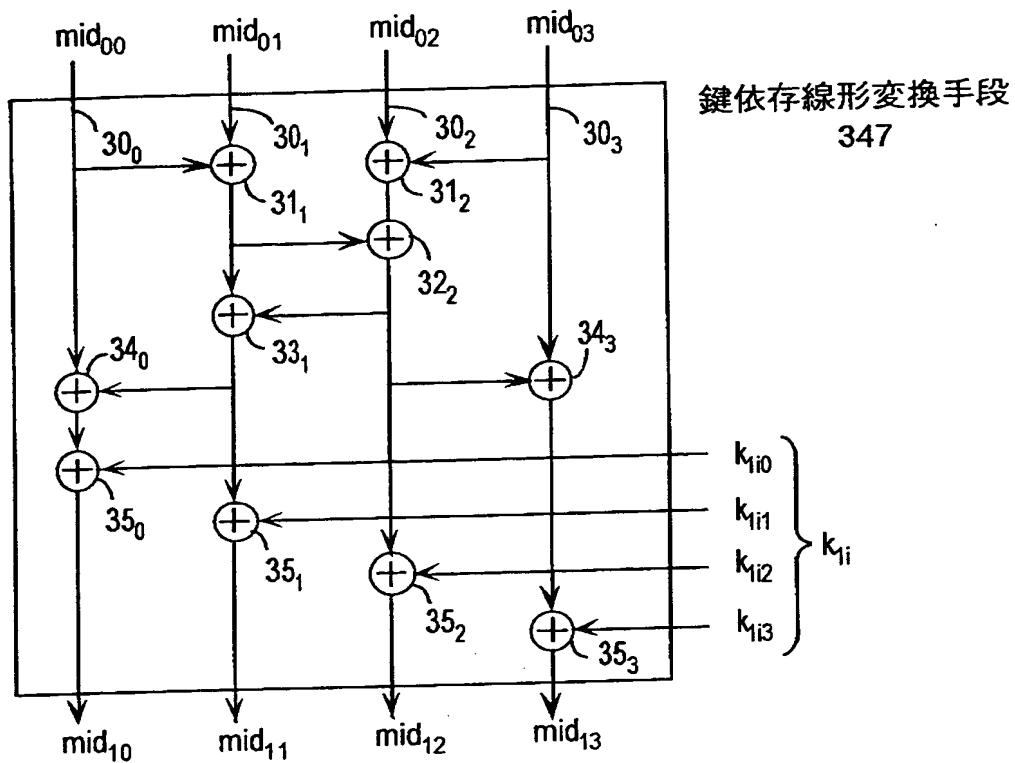


図3

【図4】

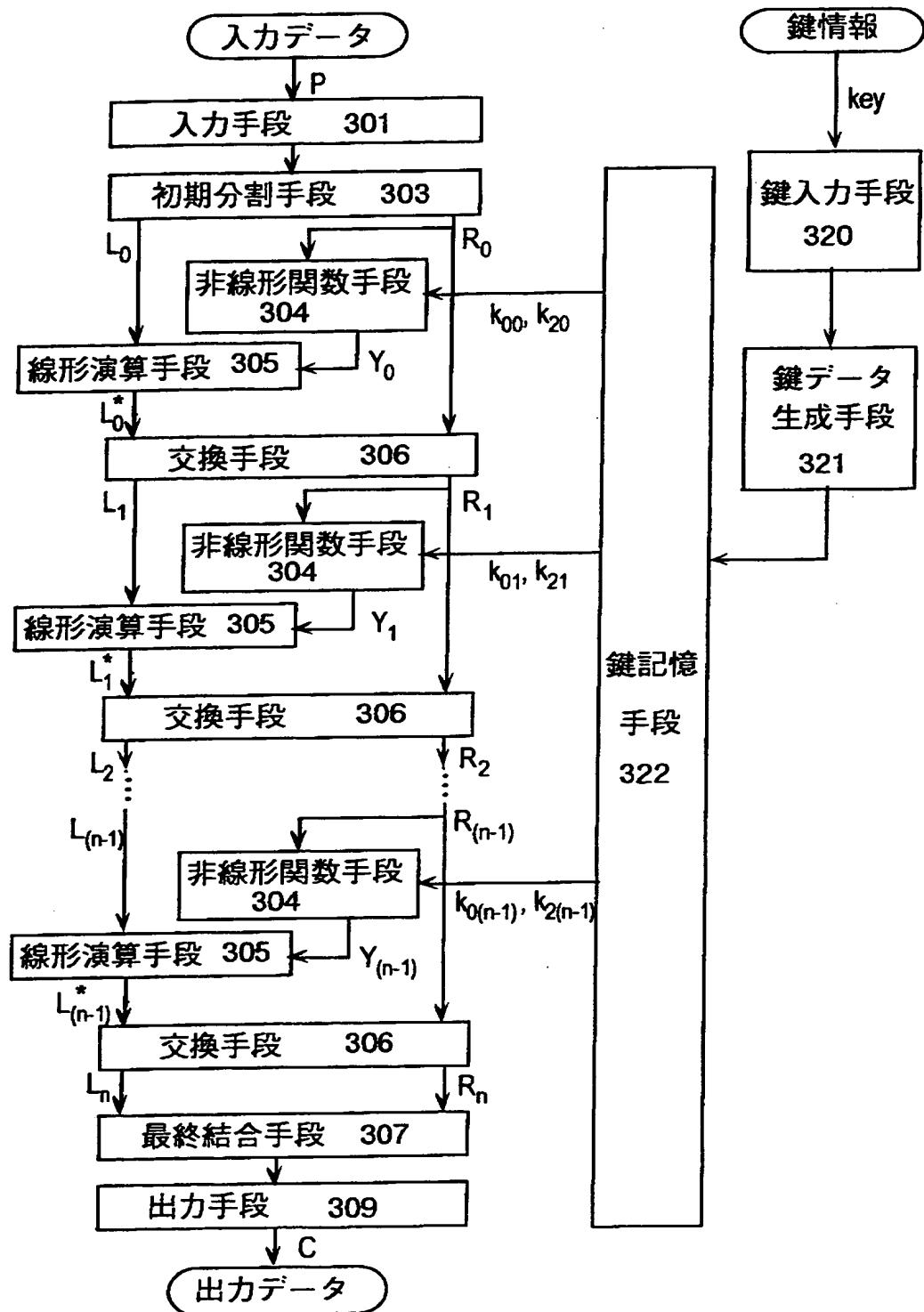


図4

【図5】

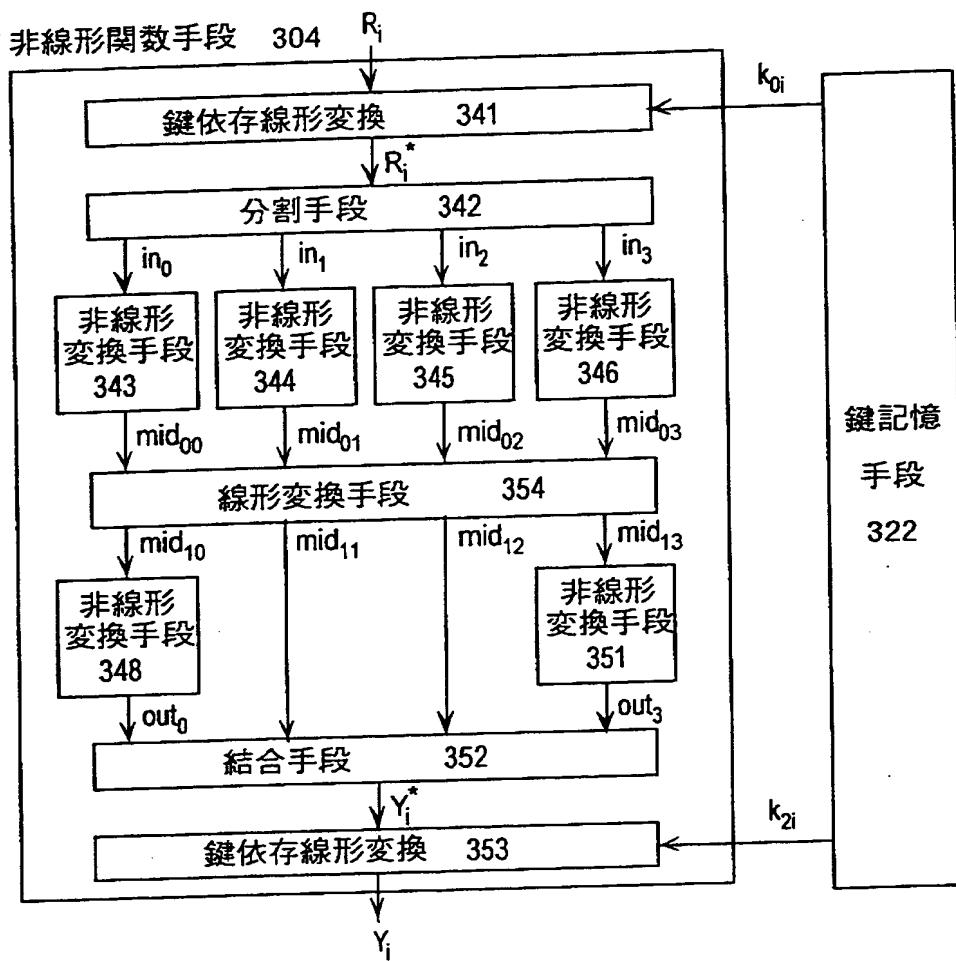


図5 A

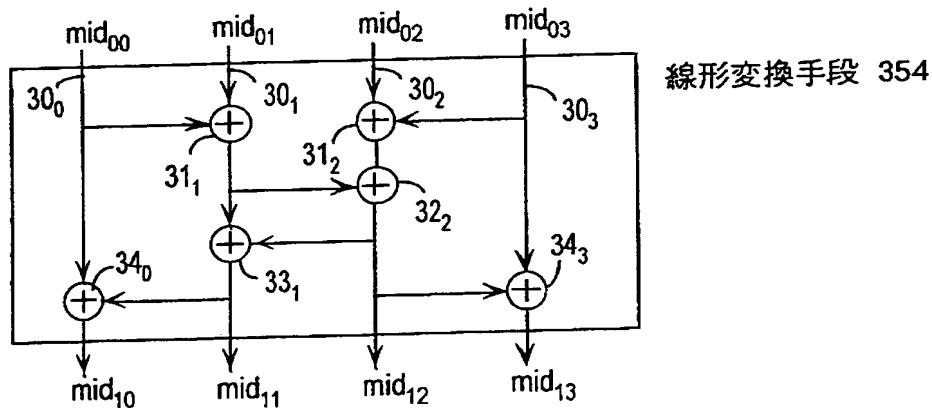


図5 B

【図 6】

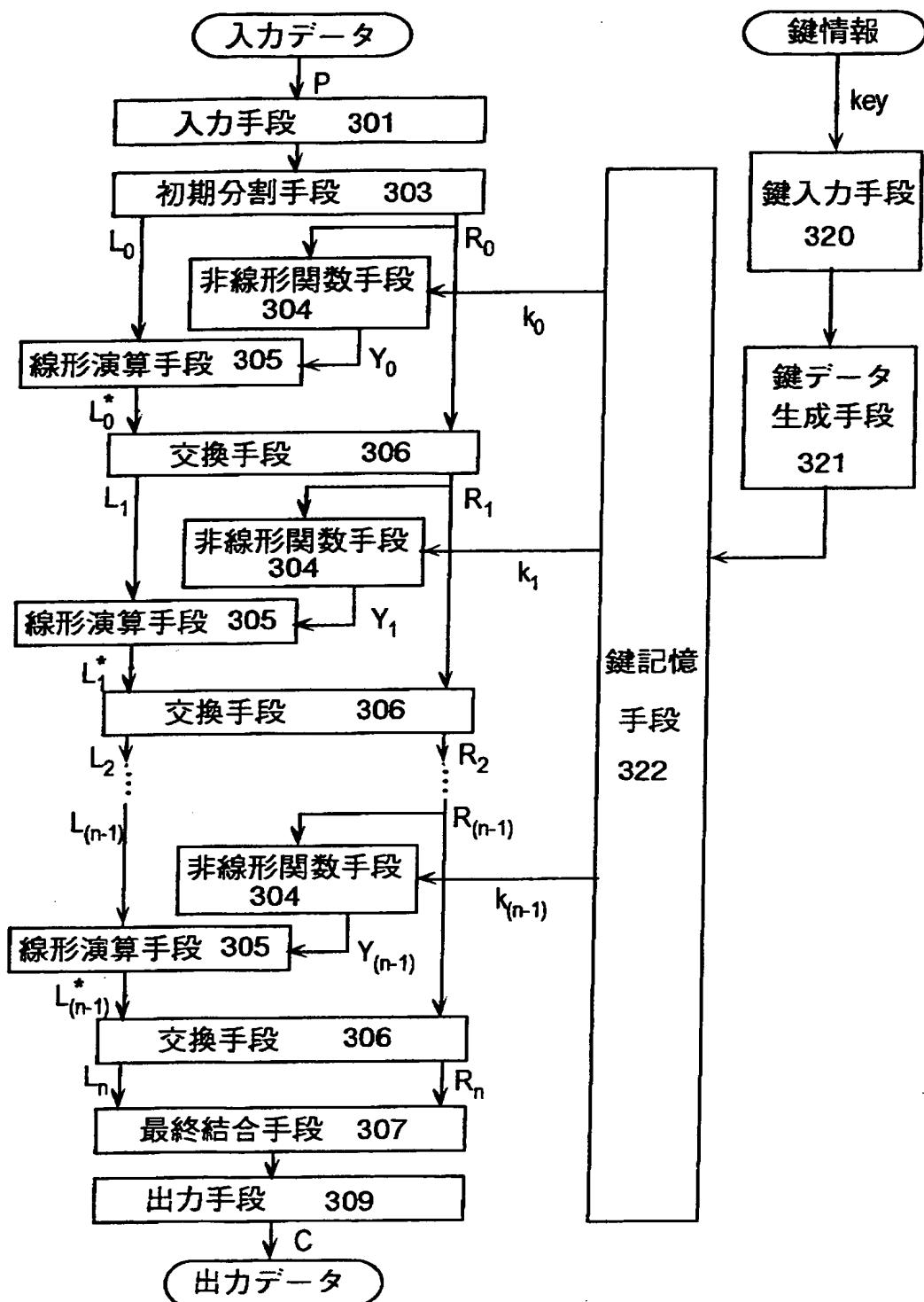


図 6

【図7】

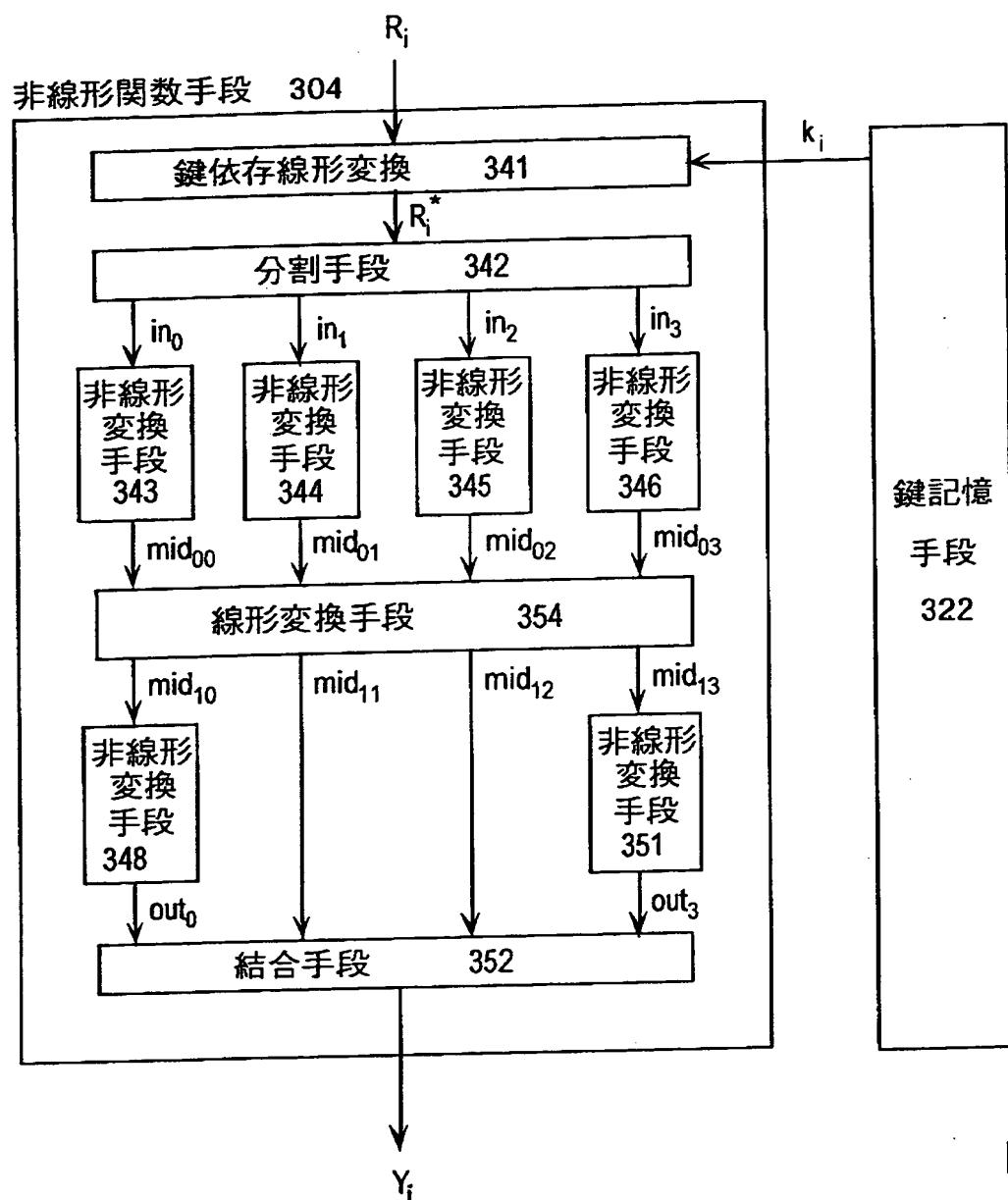


図 7

【図 8】

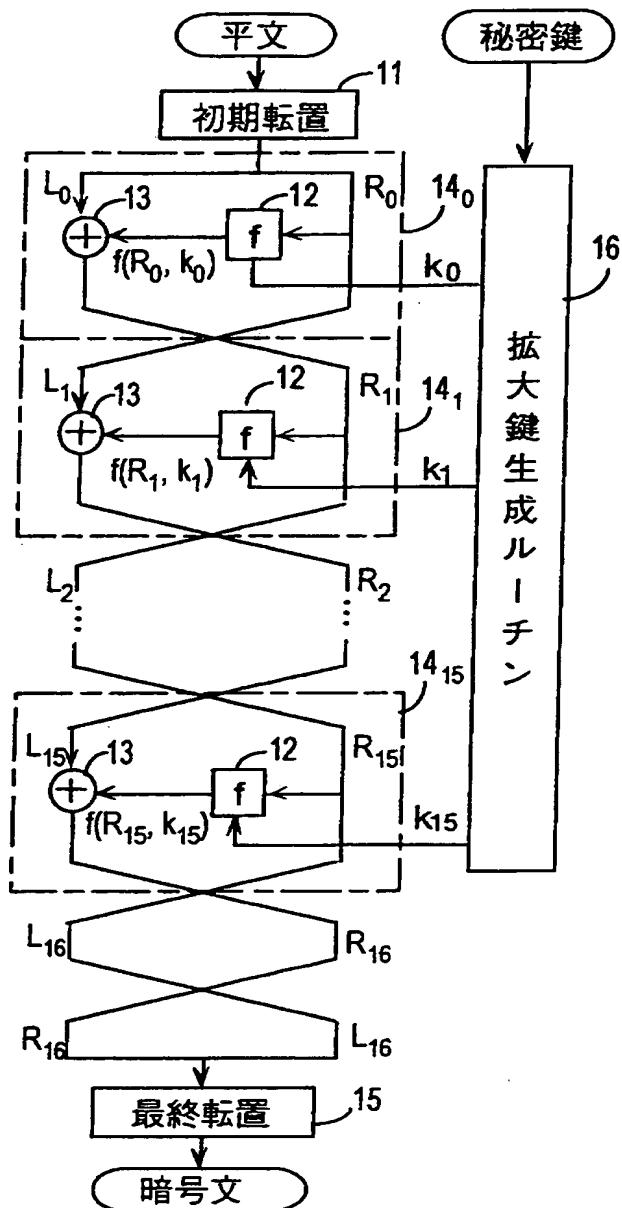


図 8

【図9】

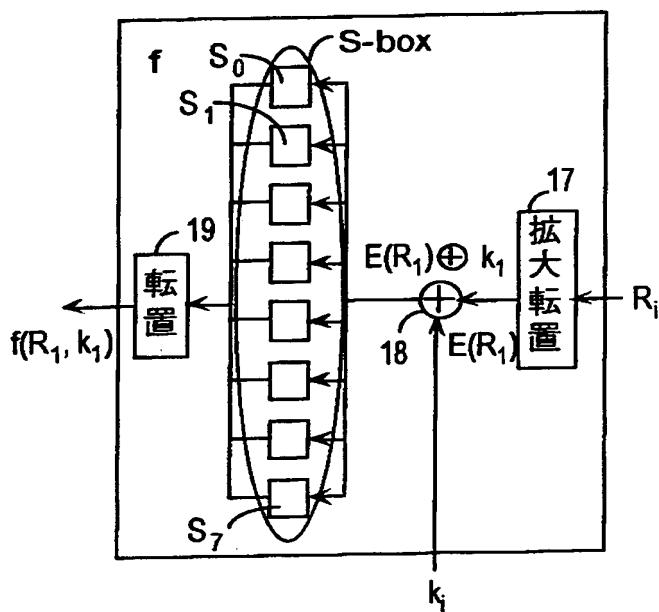


図9

【書類名】 要約書

【要約】

【課題】 差分解読法、線形解読法に対して安全性が高く、かつ高速処理が可能

【解決手段】 入力データを  $L_0$  ,  $R_0$  に分割し、 $R$  を非線形関数手段 304 で鍵に応じて交換し、その出力と、もとの排他的論理和をとった出力を  $R_1$  とし、 $R_0$  を  $L_1$  とすることを複数回行い、手段 304 として、入力  $R_i$  を鍵依存線形変換し (341) 、その出力を  $i n_0$  ,  $i n_1$  ,  $i n_2$  ,  $i n_3$  に 4 分割し、これらをそれぞれ非線形変換し (343~346) 、これら変換出力を鍵依存線形変換手段 347 で相互に関連づけると共に鍵  $k_{i0} \sim k_{i03}$  を排他的論理和をとり、その各出力をそれぞれ非線形変換し (348~351) 、その変換出力をピット結合し、更に  $k_{2i}$  で鍵依存線形変換して出力とする。

【選択図】 図 2

【書類名】 職権訂正データ  
【訂正書類】 特許願

＜認定情報・付加情報＞

【特許出願人】

【識別番号】 000004226  
【住所又は居所】 東京都新宿区西新宿三丁目19番2号  
【氏名又は名称】 日本電信電話株式会社

【特許出願人】

【識別番号】 591230295  
【住所又は居所】 東京都渋谷区桜丘町20番1号  
【氏名又は名称】 エヌティティエレクトロニクス株式会社

【代理人】

【識別番号】 100066153  
【住所又は居所】 東京都新宿区新宿四丁目2番21号 相模ビル  
【氏名又は名称】 草野 阜

出願人履歴情報

識別番号 [000004226]

1. 変更年月日 1995年 9月21日

[変更理由] 住所変更

住 所 東京都新宿区西新宿三丁目19番2号

氏 名 日本電信電話株式会社

出願人履歴情報

識別番号 [591230295]

1. 変更年月日 1991年 9月19日  
[変更理由] 新規登録  
住 所 東京都武蔵野市吉祥寺本町1丁目14番5号  
氏 名 エヌティティエレクトロニクステクノロジー株式会社

2. 変更年月日 1997年 7月24日  
[変更理由] 名称変更  
住 所 東京都渋谷区桜丘町20番1号  
氏 名 エヌティティエレクトロニクス株式会社